EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION INSTITUTE, ASBL.

Brussels, Belgium, European Union

CERTIFICATE

Artur Marek Maciag

Has successfully completed test requirements of
The European Information Technologies Certification Programme

EITC/IS/QCF Quantum cryptography fundamentals

Certification Programme examination result: 65%

Certification Programme description:

Classical approach to secure information communication: general idea of secure communication channels, private key cryptography, public key cryptography, authentication, noisy channels (errors detection, errors correction, errors detection and correction in Ethernet networks), weaknesses of classical cryptography; Unconditionally secure quantum channels conception (unconditional security of communication, Vernam cipher, One-Time-Pad cryptosystem); Quantum information: fundamental quantum information principles and postulates (definition of the qubit, the No-Cloning theorem), quantum information processing in practice; Quantum Mechanics applications towards protection of classical information; Quantum Key Distribution without use of entanglement: fundamental properties of polarized photons, Bennett and Brassard BB84 protocol, Bennett B92 protocol, Quantum Key Distribution with use of entanglement: quantum entanglement and quantum measurement outcomes correlations, EPR paradox, Bell inequalities violation, CHSH inequality violation, entanglement based Ekert E91 protocol; QKD secured communication channels: potential attacks on the quantum key distribution scheme, quantum channels with noise, privacy amplification (PA), authentication, complete scheme of secure communication, theoretical security analysis and assessment; Practical quantum cryptography implementations: QKD systems prototypes (MagiQ, idQuantique), DARPA quantum network (network structure, implementing technologies, software network layer, IPsec protocol extensions towards integration with the QKD by means of IKE implementation), European Framework Programme SECOQC project (integration of different QKD technological implementations), standardization, commercial solutions and their applications; Other applications of quantum mechanics in cryptography: bit commitment and quantum coin tossing, quantum random numbers generators, alternative ways of implementing eavesdropping proof communication channels (Kish protocol), future and perspectives of quantum cryptography

Certificate Programme version/revision: EITC/IS/QCFv1r2

CERTIFICATE ID: **EITC/IS/QCF/ERF/15004715**

To validate authenticity of this certificate or review its programme and test results scan/click QR code or visit:
www.eitci.org/validate

DATE OF ISSUE:
December 2015
Brussels, Belgium
European Union